



[Subscribe \(Full Service\)](#) [Register \(Limited Service\)](#),  
**Search:**  The ACM Digital Library  The Guide  
 +netflow +intrusion

THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satisfy](#)

## Terms used netflow intrusion

Found

Sort results by relevance   
 Display results expanded form

Save results to a Binder  
 Search Tips  
 Open results in a new window

Try an [Advanced Search](#)  
 Try this search in [The Guide](#)

Results 1 - 20 of 27

Result page: **1** [2](#) [next](#)

Relevan

- [1 VizSEC link analysis session: VisFlowConnect: netflow visualizations of link re](#)  
for security situational awareness  
 Xiaoxin Yin, William Yurcik, Michael Treaster, Yifan Li, Kiran Lakkaraju  
October 2004 Proceedings of the 2004 ACM workshop on Visualization and da  
for computer security

Full text available: [pdf\(1.51 MB\)](#) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

We present a visualization design to enhance the ability of an administrator to detect and investigate anomalous traffic between a local network and external domains. Centrally, the design is a parallel axes view which displays NetFlow records as links between two or more domains while employing a variety of visual cues to assist the user. We describe filtering options that can be employed to hide uninteresting or innocuous traffic such that the user can focus his or her attention ...

**Keywords:** link analysis, link relationships, netflows, parallel axes, parallel coordinate, security, security visualization, situational awareness

- 2** [VizSEC state analysis session: NVisionIP: netflow visualizations of system sta](#)  
security situational awareness

Kiran Lakkaraju, William Yurcik, Adam J. Lee

October 2004 Proceedings of the 2004 ACM workshop on Visualization and da  
for computer security

Full text available: [pdf\(693.53 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

The number of attacks against large computer systems is currently growing at a rapid rate. Despite the best efforts of security analysts, large organizations are having trouble keeping up with the top of the current state of their networks. In this paper, we describe a tool called NVisionIP that is designed to increase the security analyst's situational awareness. As humans are inherently visual beings, NVisionIP uses a graphical representation of a class-B network to allow analysts to quickly visualize ...

**Keywords:** NetFlows, security system state, security visualization, situational awa

### 3 Building a better NetFlow

Cristian Estan, Ken Keys, David Moore, George Varghese

August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings  
2004 conference on Applications, technologies, architectures, ai  
protocols for computer communications**, Volume 34 Issue 4

Full text available: [pdf\(256.44 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

Network operators need to determine the composition of the traffic mix on links w~~t~~ for dominant applications, users, or estimating traffic matrices. Cisco's NetFlow has into a solution that satisfies this need by reporting flow records that summarize a s the traffic traversing the link. But sampled NetFlow has shortcomings that hinder tl and analysis of traffic data. First, during flooding attacks router memory and netwc bandwidth consumed by flow records ...

**Keywords:** data summarization, network monitoring, traffic measurement

### 4 Algorithms: Bitmap algorithms for counting active flows on high speed links

Cristian Estan, George Varghese, Mike Fisk

October 2003 **Proceedings of the 3rd ACM SIGCOMM conference on Internet  
measurement**

Full text available: [pdf\(330.81 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

This paper presents a family of bitmap algorithms that address the problem of cou number of distinct header patterns (flows) seen on a high speed link. Such countin used to detect DoS attacks and port scans, and to solve measurement problems. C especially hard when processing must be done within a packet arrival time (8 nsec speeds) and, hence, must require only a small number of accesses to limited, fast i naive solution that maintains a hash table r ...

**Keywords:** counting flows, network traffic measurement

### 5 Measurement tools: Packet trace manipulation framework for test labs

Andy Rupp, Holger Dreger, Anja Feldmann, Robin Sommer

October 2004 **Proceedings of the 4th ACM SIGCOMM conference on Internet  
measurement**

Full text available: [pdf\(164.63 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

Evaluating network components such as network intrusion detection systems, firew routers, or switches suffers from the lack of available network traffic traces that on hand are appropriate for a specific test environment but on the other hand have th

characteristics as actual traffic. Instead of just capturing traffic and replaying the traces, we identify a set of packet trace manipulation operations that enable us to generate a trace bottom-up: our trace primitives can be used to ...

**Keywords:** evaluation, measurement, network, network intrusion detection, trace

**6 Computer security (SEC): Towards multisensor data fusion for DoS detection**

Christos Siaterlis, Basil Maglaris

March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**

Full text available:  [pdf\(276.26 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

In our present work we introduce the use of data fusion in the field of DoS anomaly detection. We present Dempster-Shafer's Theory of Evidence (D-S) as the mathematical foundation for the development of a novel DoS detection engine. Based on a data fusion paradigm, we combine multiple evidence generated from simple heuristics to feed our D-S inference engine and attempt to detect flooding attacks. Our approach has as its main advantages the power of Theory of Evidence in expressing beliefs and the ability to handle uncertainty ...

**Keywords:** Denial of Service, anomaly detection, data fusion

**7 Late breaking results: posters: A user-centered approach to visualizing network intrusion detection**

John R. Goodall, A. Ant Ozok, Wayne G. Lutters, Penny Rheingans, Anita Komlodi

April 2005 **CHI '05 extended abstracts on Human factors in computing system**

Full text available:  [pdf\(420.66 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

Intrusion detection (ID) analysts are charged with ensuring the safety and integrity of high-speed computer networks. Their work includes the complex task of searching for indications of attacks and misuse in vast amounts of network data. Although there are many information visualization tools to support ID, few are grounded in a thorough understanding of the work ID analysts perform or include any empirical evaluation. We present a user-centered visualization based on our understandings ...

**Keywords:** information visualization, intrusion detection, network security, usability, user-centered design

**8 Passive measurements: Characteristics of network traffic flow anomalies**

Paul Barford, David Plonka

November 2001 **Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement**

Full text available:  [pdf\(2.94 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [terms](#)

**9 Detection: Characterization of network-wide anomalies in traffic flows**

Anukool Lakhina, Mark Crovella, Christophe Diot

**October 2004 Proceedings of the 4th ACM SIGCOMM conference on Internet measurement**Full text available: [pdf\(125.66 KB\)](#)Additional Information: [full citation](#), [abstract](#), [reference terms](#)

Detecting and understanding anomalies in IP networks is an open and ill-defined problem. Toward this end, we have recently proposed the subspace method for anomaly detection. In this paper we present the first large-scale exploration of the power of the subspace method when applied to flow traffic. An important aspect of this approach is that it fuses information from flow measurements taken throughout a network. We apply the subspace method to different types of sampled flow traffic in ...

**Keywords:** anomaly detection, network traffic analysis**10 Session 5: P2P and streaming: Analyzing peer-to-peer traffic across large networks**

Subhabrata Sen, Jia Wang

**November 2002 Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement**Full text available: [pdf\(1.56 MB\)](#)Additional Information: [full citation](#), [abstract](#), [reference terms](#), [index terms](#)

The use of peer-to-peer (P2P) applications is growing dramatically, particularly for large video/audio files and software. In this paper, we analyze P2P traffic by measuring level information collected at multiple border routers across a large ISP network, aiming our investigation of three popular P2P systems -- FastTrack, Gnutella, and DirectConnect. We characterize the P2P traffic observed at a single ISP and its impact on the underlying network. We observe very skewed distribution ...

**11 Networks applications: Gigoscope: high performance network monitoring with a graphical user interface**

Chuck Cranor, Yuan Gao, Theodore Johnson, Vlaidslav Shkapenyuk, Oliver Spatscheck

**June 2002 Proceedings of the 2002 ACM SIGMOD international conference on Management of data**Full text available: [pdf\(108.27 KB\)](#)Additional Information: [full citation](#), [abstract](#), [citations](#), [journal](#)

Operators of large networks and providers of network services need to monitor and analyze the network traffic flowing through their systems. Monitoring requirements range from long term (e.g., monitoring link utilizations, computing traffic matrices) to the ad-hoc (detecting network intrusions, debugging performance problems). Many of the applications are complex (e.g., reconstruct TCP/IP sessions), query layer-7 data (find streaming media connections), operate over huge volumes of data ...

**12 Identification and classification: Online identification of hierarchical heavy hitters: algorithms, evaluation, and applications**

Yin Zhang, Sumeet Singh, Subhabrata Sen, Nick Duffield, Carsten Lund  
~~October 2004 Proceedings of the 4th ACM SIGCOMM conference on Internet measurement~~

Full text available: [pdf\(273.81 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [reference terms](#)

In traffic monitoring, accounting, and network anomaly detection, it is often important to detect high-volume traffic clusters in near real-time. Such heavy-hitter traffic are often hierarchical (<i>e.g.</i>, they may occur at different aggregation levels like IP addresses) and possibly multidimensional (<i>e.g.</i>, they may involve the correlation of different IP header fields like IP addresses, port numbers, and protocol). Without prior knowledge about ...

**Keywords:** change detection, data stream computation, hierarchical heavy hitters, anomaly detection, packet classification

### 13 Detection: Reversible sketches for efficient and accurate change detection over data streams

Robert Schwellner, Ashish Gupta, Elliot Parsons, Yan Chen

~~October 2004 Proceedings of the 4th ACM SIGCOMM conference on Internet measurement~~

Full text available: [pdf\(161.14 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [reference terms](#)

Traffic anomalies such as failures and attacks are increasing in frequency and severity, thus identifying them rapidly and accurately is critical for large network operators. Current detection typically treats the traffic as a collection of flows and looks for heavy chain traffic patterns (<i>e.g.</i>, volume, number of connections). However, as link speed increases, the number of flows increase, keeping per-flow state is not scalable. The recently proposed sketch-based schemes [14] are ...

**Keywords:** IP mangling, change detection, data stream computation, modular hash, network anomaly detection, reverse hashing, sketch

### 14 Session 3: inference and statistical analysis: A signal analysis of network traffic anomalies

Paul Barford, Jeffery Kline, David Plonka, Amos Ron

~~November 2002 Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement~~

Full text available: [pdf\(1.52 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

Identifying anomalies rapidly and accurately is critical to the efficient operation of computer networks. Accurately characterizing important classes of anomalies greatly facilitates their identification; however, the subtleties and complexities of anomalous traffic can confound this process. In this paper we report results of signal analysis of four classes of network traffic anomalies: outages, flash crowds, attacks and measurement failure.

this study consists of IP flow ...

## 15 Structural analysis of network traffic flows

Anukool Lakhina, Konstantina Papagiannaki, Mark Crovella, Christophe Diot, Eric D. K Nina Taft

June 2004 ACM SIGMETRICS Performance Evaluation Review , Proceedings o international conference on Measurement and modeling of computer systems, Volume 32 Issue 1

Full text available: [pdf\(628.43 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

Network traffic arises from the superposition of Origin-Destination (OD) flows. A thorough understanding of OD flows is essential for modeling network traffic, and for addressing a wide variety of problems including traffic engineering, traffic matrix estimation, capacity planning, forecasting and anomaly detection. However, to date, OD flows have been closely studied, and there is very little known about their properties. We present an analysis of complete sets of OD flow time-series ...

**Keywords:** network traffic analysis, principal component analysis, traffic engineering



## 16 Detection: On scalable attack detection in the network

Ramana Rao Komella, Sumeet Singh, George Varghese

October 2004 Proceedings of the 4th ACM SIGCOMM conference on Internet measurement

Full text available: [pdf\(405.42 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

Current intrusion detection and prevention systems seek to detect a wide class of network intrusions (e.g., DoS attacks, worms, port scans) at network vantage points. Unfortunately the IDS systems we know of keep per-connection or per-flow state. Thus it is hard to believe that IDS systems (other than signature detection mechanisms) have scaled to gigabit speeds. By contrast, note that both router lookups and fair queuing have scaled to speeds using <i>aggregation</i> ...

**Keywords:** denial of service, scalability, security

## 17 Session 9: traffic analysis: Agile and scalable analysis of network events

Mike Fisk, George Varghese

November 2002 Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement

Full text available: [pdf\(731.48 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

The state of the art in general purpose software systems for large-scale traffic measurement has not progressed much past the venerable *libpcap*. In this paper we describe a new analysis system that provides a scalable, flexible system for composing ad-hoc analysis of high-speed, streaming data. This agility allows researchers, network security analysts,

network operators to easily compose new analysis functions. A growing tool box of measurement, and statistical tools al ...

## 18 Session 3: Toward understanding distributed blackhole placement

Evan Cooke, Michael Bailey, Z. Morley Mao, David Watson, Farnam Jahanian, Danny T  
October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode**

Full text available:  [pdf\(478.95 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference terms](#)

The monitoring of unused Internet address space has been shown to be an effective for characterizing Internet threats including Internet worms and DDOS attacks. Because no legitimate hosts in an unused address block, traffic must be the result of misconfiguration, backscatter from spoofed source addresses, or scanning from two other probing. This paper extends previous work characterizing traffic seen at specific address blocks by examining differences observed b ...

**Keywords:** blackhole monitoring, blackhole placement, computer worms, globally threats, internet motion sensor, network security

## 19 DOS protection: Hop-count filtering: an effective defense against spoofed DDoS

Cheng Jin, Haining Wang, Kang G. Shin

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Full text available:  [pdf\(213.86 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

IP spoofing has been exploited by Distributed Denial of Service (DDoS) attacks to (1) flooding sources and localities in flooding traffic, and (2) coax legitimate hosts into reflectors, redirecting and amplifying flooding traffic. Thus, the ability to filter spoofed packets near victims is essential to their own protection as well as to their avoidance of becoming involuntary DoS reflectors. Although an attacker can forge any field in the header or she cannot falsify t ...

**Keywords:** DDoS defense, TTL, host-based, networking, security

## 20 Approximations: Sketch-based change detection: methods, evaluation, and applications

Balachander Krishnamurthy, Subhabrata Sen, Yin Zhang, Yan Chen

October 2003 **Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement**

Full text available:  [pdf\(309.23 KB\)](#) Additional Information: [full citation](#), [abstract](#), [reference index terms](#)

Traffic anomalies such as failures and attacks are commonplace in today's network. Identifying them rapidly and accurately is critical for large network operators. The current approach typically treats the traffic as a collection of flows that need to be examined for significant changes in traffic pattern (eg, volume, number of connections). However, as link speed increases and the number of flows increase, keeping per-flow state is either too expensive or too

propose building compact summaries of ...

**Keywords:** change detection, data stream computation, forecasting, network anor detection, sketch, time series analysis

Results 1 - 20 of 27

Result page: [1](#) [2](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 AC  
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real I](#)

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

 [Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE XPORE GUIDE](#)

e-mail

Results for "(netflow &lt;and&gt; intrusion&lt;in&gt;metadata)"

Your search matched 8 of 1157693 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.[» View Session History](#)[» New Search](#)[Modify Search](#)[» Key](#)

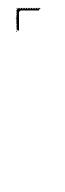
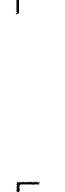
IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

[Select](#)   [Article Information](#)1. **NetFlow based intrusion detection system**Tsang-Long Pao; Po-Wei Wang;  
Networking, Sensing and Control, 2004 IEEE International Conference on  
Volume 2, 2004 Page(s):731 - 736 Vol.2[AbstractPlus](#) | Full Text: [PDF\(1568 KB\)](#) IEEE CNF2. **Log correlation for intrusion detection: a proof of concept**Abad, C.; Taylor, J.; Sengul, C.; Yurcik, W.; Zhou, Y.; Rowe, K.;  
Computer Security Applications Conference, 2003. Proceedings. 19th Annual  
8-12 Dec. 2003 Page(s):255 - 264[AbstractPlus](#) | Full Text: [PDF\(285 KB\)](#) IEEE CNF3. **Extracting Attack Manifestations to Determine Log Data Requirements for Intrusi**Barse, E.L.; Jonsson, E.;  
Computer Security Applications Conference, 2004. 20th Annual  
06-10 Dec. 2004 Page(s):158 - 167[AbstractPlus](#) | Full Text: [PDF\(176 KB\)](#) IEEE CNF4. **Inbound traffic engineering for multihomed ASs using AS path prepending**Chang, R.K.C.; Lo, M.;  
Network, IEEE  
Volume 19, Issue 2, March-April 2005 Page(s):18 - 25[AbstractPlus](#) | Full Text: [PDF\(539 KB\)](#) IEEE JNL5. **Honeypot forensics part 1: analyzing the network**Raynal, F.; Berthier, Y.; Biondi, P.; Kaminsky, D.;  
Security & Privacy Magazine, IEEE  
Volume 2, Issue 4, July-Aug. 2004 Page(s):72 - 78[AbstractPlus](#) | Full Text: [PDF\(168 KB\)](#) IEEE JNL6. **Enlisting event patterns for cyber battlefield awareness**Perrochon, L.; Eunhei Jang; Kasriel, S.; Luckham, D.C.;  
DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proce  
Volume 2, 25-27 Jan. 2000 Page(s):411 - 422 vol.2[AbstractPlus](#) | Full Text: [PDF\(148 KB\)](#) IEEE CNF

7. A scalable high performance network monitoring agent for CERNET  
Zhang Hui; Li Xing; Li Zimu;  
Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003:  
the Fourth International Conference on  
27-29 Aug. 2003 Page(s):151 - 156

[AbstractPlus](#) | Full Text: [PDF\(498 KB\)](#) IEEE CNF

8. Facilitating interactive distributed data stream processing and mining  
Ghoting, A.; Srinivasan Parthasarathy;  
Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International  
26-30 April 2004 Page(s):86

[AbstractPlus](#) | Full Text: [PDF\(2603 KB\)](#) IEEE CNF



[Help](#) [Contact Us](#) [Privacy & S](#)

© Copyright 2005 IEEE –

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

 [Search Session History](#)[BROWSE](#)[SEARCH](#)[IEEE XPORE GUIDE](#)

Edit an existing query or  
compose a new query in the  
Search Query Display.

Tue, 17 May 2005, 1:33:56 PM EST

**Search Query Display** 

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

**Recent Search Queries**

- |    |  |
|----|--|
| #1 | ((netflow & intrusion)<in>metadata)) & (pyr >= 1950 & pyr <= 2000) |
| #2 | (NETFLOW & INTRUSION<IN>metadata)                                  |
| #3 | (NETFLOW & INTRUSION<IN>metadata)                                  |

[Help](#) [Contact Us](#) [Privacy & S](#)

© Copyright 2005 IEEE -

Indexed by  
 Inspec®



The Swiss Education &amp; Research Network



## FloMA: Pointers and Software

### Network

**Maps**  
**Operations**  
**Services**  
**Projects**  
 IPv6  
 SWITCHlambda  
 Sequin  
 TF-NGN  
 TTM  
 Performance

### FloMA: Software

#### Pointer Collections

[FreshMeat NetFlow projects](#)

A list of pointers to open-source projects related to NetFlow.

[Internet Tools Taxonomy](#)

On CAIDA's Web server. Includes many traffic analysis tools.

[NetFlow Applications list](#)

On InMon's Web server.

[Cisco NetFlow Ecosystem Solutions](#)

Contains descriptions of many applications that integrate NetFlow support, n commercial software with the exception of [FlowScan](#) and [flow-tools](#).

#### NetFlow

[FlowScan](#)

A Perl-based system to analyze and report on flows collected by [flow-tool](#) [cflowd](#), by Dave Plonka. Sample output graphs are available too, as well as Majordomo-driven mailing lists for announcements and general discussion (is currently built on [Cflow.pm](#). User-contributed tools based on FlowScan in [CarrierIn](#) from Stanislav Sinyagin

which claims to be more suitable for larger ISP/Carriers

[CUFlow](#) from Matt Selsky and Johan M. Andersen at Columbia University which is an alternative graphing tool "designed to combine the features of CampusIO and SubNetIO". Robert S. Galloway has contributed a nice style document describing how it can be used.

[FlowMonitor](#) from Johan M. Andersen at Columbia University

monitors individual users' network usage against a bandwidth usage

[JKFlow](#) by Jurgen Kobierczynski

A new reporting module which is highly configurable using an XML configuration file.

[flow-tools](#)

Similar to [cflowd](#) but implemented as a set of smaller tools, with the addition of compression of the recorded data, thus capable of recording many more flows than [cflowd](#) without using a lot of disk space. See [paper](#) about its application for Intrusion Detection or also a mailing list for the package.

There is a short presentation called [Ohio Gigapop Traffic Measurements](#) that shows some examples on how flow-tools can be used.

The package is widely used, and there are quite a few user contributions, such as [flow-extract](#), which can be used to filter flow-tools-recorded flows through specified tests; a set of "[Inter.netPH contribs](#)" by Horatio B. Bogbindero; some patches and a [Python module](#) by Robin Sommer.

[Stager](#)

Stager is a system for aggregation and presentation of network statistics from flow-tools package. Includes PostgreSQL storage of aggregated statistics, as well as a simple frontend. A public [demo](#) is available.

[CESNET NetFlow Monitor](#)

by Jan Nejman.

RUS-CERT tools

The CERT of the Stuttgart University computing center (RUS-CERT) has published tools that they use internally to analyze Netflow data. Some of the documents are in German.

pmacct [NEW]

A set of tools to account and aggregate IP traffic. Originally based on libpcap, it now supports Netflow v1 and v5, and should soon support Netflow v9, too.

NEye

NEye is a Netflow V5 collector. It logs incoming Netflow V5 data to ASCII, MySQL or SQLite databases, and it makes full use of POSIX threads if available. It works on major platforms (Linux, Solaris, AIX, Irix, HP/UX, Mac OS X, Digital Unix, etc.) and others too (Ultrix, Nextstep, etc.).

NetFlow2MySQL, NetFlow2XML, and pcNetFlow

Three products from a research project at the NARA Institute of Science and Technology.

F.L.A.V.I.O. (see also the [FreshMeat page](#))

A Perl-based NetFlow collector that stores flow data "into a MySQL database back to graph daily, weekly, monthly and yearly charts."

CAIDA cflowd

Rather complex system with distributed log servers. Released in 1998, this was an open-source software system to work on NetFlow data, but doesn't seem to be maintained anymore. CAIDA have prepared a nice [FAQ](#) which contains interesting information both on Cflowd and on NetFlow in general. CAIDA has announced that they no longer support cflowd, and recommend that people move to [flow-tools](#).

Fluxoscope

Software used for charging, monitoring, and traffic analysis at SWITCH. Includes own NetFlow v5 accounting receiver which aggregates traffic into multidimensional matrices (AS/site/application). Most of the software is written in Common Lisp.

UDP Samplicator

A small program that receives UDP datagrams and redistributes them to a set of receivers. Useful to distribute NetFlow accounting streams to multiple post-processing programs. Is able to distribute only a specified percentage of all packets to each receiver. Note that recent versions added the possibility of "spoofing" the source's IP address.

Panoptis

An open-source project started by Costas Kotsokalis from GRNET, the Greek Research and Education Network. Uses NetFlow accounting data to detect (Distributed) Denial of Service. *Status as of early May 2002:* Supports NetFlow v1 or v5 as inputs, with v8 (aggregated) support under development. The system is currently being extended to support attack trace-back using a mesh of detectors.

MHTG (Multi Host Traffic Grapher)

Uses NetFlow to generate per-host graphs of traffic for a campus network. Network interface implemented as a Java applet which allows interaction with traffic. Software consists of a C++ program to process NetFlow data, a MySQL backend and the Java grapher.

Matt's Quick & Dirty CFLOWD tutorial and scripts...

Postprocessing scripts for cflowd data by Matthew Petach

flow2rrd.pl

Converts a Cisco NetFlow stream into set of RRDtool files, based on set of IP addresses. By Alex Pilosov.

Slate

An application that converts LFAP data into NetFlow records - see <http://www.nmops.org/>.

Ntop

This well-known libpcap-based network usage monitor has been extended to support NetFlow v5 accounting data. It also supports sFlow.

SiLK [NEW]

SiLK, the System for Internet-Level Knowledge, is a collection of netflow tools developed by the CERT/NetSA (Network Situational Awareness) Team to facilitate security analysis in large networks.

NFDUMP

A set of tools to capture/record, dump, filter, and replay NetFlow (v5/v7) data. Filters flows according to multiple user-defined profiles.

NfSen [NEW]

Graphical Web-based front-end for the NFDUMP tools. Plots aggregate statistics over time, supports filtering and drilling down up to the individual flow level.

UPFrame

This UDP/Netflow Processing Framework is a system for real-time processing

packet streams such as Netflow export data. It features a general infrastructure dynamically configurable plugin modules,

#### nProbe

A small self-contained program that generates NetFlow accounting data for a stream sniffed off one or several interfaces. Works under Unix and Windows environments. It can be used to build inexpensive NetFlow probes.

#### fprobe (I)

Traffic probe that can generate NetFlow data. Based on the libpcap library. F implementation in C.

#### fprobe (II)

Another NetFlow-generating software traffic probe.

#### Softflowd

Traffic probe that can generate NetFlow data. Based on libpcap. Comes with collector in Perl. Both the server (probe) and client (collector) support export over IPv6. Very lean (as of June 2004) implementation in C.

The pfflowd variant is based on OpenBSD's PF interface.

#### Argus from QoSient

This network *Audit Record Generation and Utilization System* can be used for detection and QoS monitoring. It is also mentioned in the reference section on pages.

#### Flowc

"a tool for gathering, storing and analyzing traffic accounting for Cisco route NetFlow enabled switching (version 5). This package could be used by ISP for analysis and billing procedures."

#### NetFlowMet

Starting with release 4.2, Nevil Brownlee's *NeTraMet* package includes *NetFlowMet* which implements an RTFM meter fed on Netflow accounting data.

#### NetFlow Accounting software from ABPSoft

A self-contained NetFlow processing system written in C. Writes captured flow Postprocessor breaks up this data over peers according to a definition file.

#### EHNT (Extreme Happy NetFlow Tool) by Nik Weidenbacher

Another self-contained NetFlow accounting packet processor. The receiving part functions as a server to which various kinds of clients can connect. Also writes to

#### Hendrik Visage's NetFlow tools

FTP site with various tools for NetFlow postprocessing. In particular, you will find:

1. a UDP duplicator (hack of smplicator to preserve the source router IP)
2. a couple of hacks to cflowd for dumping the flows every %n seconds ("flhh" to output flowdump stuff aggregated, ready for a "grep|sed "s/.../update /" |rrdtool -"

#### MATHE

An article (in French) about a Netflow accounting and visualization system under Linux. Uses an Oracle database and Perl DBI/GD scripts to generate a nice breakdown of external traffic to departments/institutes.

#### JANET Traffic Accounting Site

An impressive application of Netflow which is used for volume-based charging of JANET's U.S. connection. Other statistics at JANET were done using NeTrameter.

#### sFlow Toolkit

Open source tools for analyzing sFlow data. Allows sFlow data to be used with other open source tools, including: tcpdump, snort and MRTG or rrdtool. Also allows to convert sFlow packets to NetFlow packets.

## **Commercial Applications**

#### Caligare Flow Inspector and NetImonitor

Analyzes NetFlow data for network monitoring as well as attack detection and prevention. Works with NetFlow data export version 1,5,6,7 and 9. NetImonitor is primarily designed for use in the United States.

#### QRadar from Q1 Labs

The system can use Netflow data, but also includes its own payload-aware flow classifier which produces bi-directional flow information in a format called QFlow.

#### Cyclades-nQuirer

A network traffic monitoring appliance that can generate data in both Netflow and sFlow formats.

#### Crannog Software's Netflow Monitor

LAN and WAN bandwidth analysis based on NetFlow data. Includes a Web interface including Java applets to display traffic graphs and to enable drill-down. As of November 2003, runs on Microsoft Windows NT4/2000/XP. An evaluation version of Netflow Monitor is now available for download. Crannog is also said to have support for Netflow version 9.

I-ABA and M-NTM from Tek Yazilim

Windows-based software to analyze NetFlow (and Cisco IP Accounting) statistics. Specifically analyzes AS-to-AS traffic streams. Trial versions can be downloaded.

Network Signature BENTO

BENTO stands for ``BGP Enabled Network Traffic Organizer'' and is a high-performance NetFlow data processor with an integrated BGP-4 implementation to facilitate analysis based on complex external routing relationships. Product offerings include a software/support package and an ``appliance'' consisting of a preconfigured rack-mount server.

IsarFlow from IsarNet

IsarFlow is a traffic analysis tool for accounting, capacity planning, QoS monitoring and application distribution within Citrix sessions based on Netflow.

NetQoS ReporterAnalyzer

Scalable solution for the visualization of network traffic data

ManageEngine NetFlow Analyzer [NEW]

from AdventNet. Supports location of bottlenecks and allows drilling down to determine what is causing them. Thirty-day evaluation license available free of charge. Available on Windows, Linux (x86) and Solaris (SPARC).

NetUsage from Apoapsis (formerly called WANBUS)

The NetUsage suite strives to provide visibility of network traffic, producing reports not only for network professionals, but for IT management, business and accounts departments. Supports network traffic monitoring, capacity planning, business justification and cost control.

Apogee Networks

The NetCountant network usage-based billing system and the NetScope real-time network monitoring and performance analysis solution support NetFlow, RMON, RADIUS, other SNMP MIBs, and ``Layer 7'' application/content switches.

Nazca.Billing

Integrated billing software for "Telephony, Internet and Networks". Contains interfaces to many accounting systems including NetFlow.

Arbor Networks

Peakflow DOS detects denial-of-service attacks, and Peakflow Traffic analyzer tracks and routing history. Both can process NetFlow accounting data. As of November 2004, Arbor is said to support Netflow v9.

CiscoNetFlow FlowCollector/Network Data Analyzer

Similar to cfloodd but productized, with a (Java-based) GUI and possibly better possibilities of defining filters and aggregation schemes.

- [NetFlow Collector 3.6 documentation](#), demo version [download](#)

- [Network Data Analyzer 3.6 documentation](#), demo version (3.0) [download](#)

NAM (Network Analyzer Module)

This is a "NetFlow collector on a linecard" for the Catalyst 6500/7600 OSR platform.

Concord

Network Health uses NetFlow and RMON2 accounting information ``to determine application, bandwidth and server usage.''

Digiquant

IMS accounting and billing system based on Oracle 9i under Unix.

Quallaby

Has a Netflow application package for its PROVISO system for network performance monitoring and service assurance.

Gadgets Software & Professional Services Ltd.

Network Intelligence traffic measurement and visualisation software for GNU/Linux and Windows (client only) platforms. Free trial available. Includes 3D visualizations using OpenGL.

The author also wrote [bbnfc](#), a ``bare-bones Netflow collector tool'' that simply receives and displays Netflow v5 packets.

Hewlett-Packard

The Smart Internet Billing Solution usage management system and well as the Performance Insight for Networks (OVPI) use NetFlow accounting data as part of their products.

InfoVista Corporation

InfoVista Service Level Management (SLM) and conformance solution.

InMon Traffic Server

is a commercial, web-based application running on Linux that provides real-time and historical analysis of flow information from sFlow and NetFlow sources. Web interface provides easy access to historical traffic matrices. Real-time top talker charts and sources of congestion.

Ixia

IxTraffic integrates NetFlow accounting data with topology information from multiple feeds to allow analysis of inter-domain traffic patterns.

Micromuse

*Cisco Info Center USM* ``acquires, analyzes, displays and exports Internet traffic information.

NARUS

*OSS Mediation solutions*

NetScout

*nGenius Performance Manager* ``is a complete solution for proactive monitoring, troubleshooting, capacity planning, and Voice over IP (VoIP) monitoring".

Portal Software

*Infranet* real-time customer management and billing software.

RODOPI

Billing software for ISPs.

XACCT

Commercial vendor of accounting and billing solutions with the ability to process (among others) Netflow accounting data

LoriotPro

A network monitoring ("supervision" in franglais) system that includes a NetFlow meter.

**RTFM**

Currently, there are a few implementations of RTFM meters:

NeTraMet and NetFlowMet by Nevil Brownlee of the University of Auckland.

NeTraMet is based on traffic snooping and runs on Intel PCs and several types of workstation. NetFlowMet gathers Netflow accounting information from (Cisco) routers and makes that available in RTFM-compatible.

IBM

IBM is supposed to have implemented the RTFM framework, but I couldn't find any references to this work.

**For updates and additions to this page, please contact [simon@switch.ch](mailto:simon@switch.ch).**